7. What are the differences between a TCP Connect Scan and a SYN Scan ?

The **TCP Connect Scan** and the **SYN Scan** are two common techniques used in network scanning with tools like Nmap. Here are the key differences between the two:

1. Connection Method

- **TCP Connect Scan (`-sT`):**
  - Establishes a full TCP connection with the target port by completing the three-way handshake (SYN, SYN-ACK, ACK).
  - This means that it actively connects to the target service, which can be easily logged by intrusion detection systems (IDS) and firewalls.
- **SYN Scan (`-sS`):**
  - Sends only a SYN packet to the target port to initiate the connection.
  - If the port is open, the target responds with a SYN-ACK, and if it is closed, it replies with a RST (reset) packet.
  - The scan does not complete the handshake, making it stealthier and less likely to be logged by the target.

2. Stealth Level

- **TCP Connect Scan:**
  - Less stealthy since it completes the handshake, which can be logged by the target's firewall or IDS.
  - Can be detected by network monitoring systems, making it easier for administrators to notice the scan.
- **SYN Scan:**
  - More stealthy because it does not establish a full connection. It is often referred to as a "half-open" scan.
  - Less likely to be logged because it doesn't complete the connection, which can help avoid detection by security systems.

3. Response Handling

- **TCP Connect Scan:**
  - If the port is open, a successful connection is established, and the scanner can interact with the service.
  - It will typically close the connection immediately after receiving the response.

- **SYN Scan:**
    - The scanner only needs to receive the SYN-ACK (for open ports) or RST (for closed ports) to determine the port's state.
    - No interaction with the service occurs beyond the initial SYN packet.

4. Performance

- **TCP Connect Scan:**
    - Generally slower than a SYN scan because it establishes a full connection for each open port and can be affected by timeouts.
    - More resource-intensive on both the scanning and the target system due to the full connection process.
- **SYN Scan:**
    - Typically faster and more efficient, especially when scanning multiple ports or a large number of hosts.
    - Can also use timing options to further increase performance without overwhelming the target.

5. Use Cases

- **TCP Connect Scan:**
    - Useful when stealth is not a primary concern, such as when permission is obtained for testing or when a complete connection is required to test a service.
    - Often used in scenarios where firewalls and security measures are less stringent.
- **SYN Scan:**
    - Preferred in penetration testing and security assessments where stealth is crucial.
    - Ideal for quickly identifying open ports without triggering security alarms.

Example Commands

- **TCP Connect Scan:**

    ```
    nmap -sT <target>
    ```

- **SYN Scan:**

    ```
    nmap -sS <target>
    ```

Conclusion

In summary, the main differences between a TCP Connect Scan and a SYN Scan revolve around the connection method, stealth level, response handling, performance, and use cases. The SYN Scan is generally favored for its stealth and speed, while the TCP Connect Scan can be more straightforward but less discreet.